



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/931,151	08/17/2001	Virgil Dorin Gligor	068398-0107	3167
22428	7590	10/06/2005		
FOLEY AND LARDNER SUITE 500 3000 K STREET NW WASHINGTON, DC 20007			EXAMINER JUNG, DAVID YIUK	
			ART UNIT	PAPER NUMBER
			2134	

DATE MAILED: 10/06/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/931,151	Applicant(s) GLIGOR ET AL.	
	Examiner David Y. Jung	Art Unit 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 03 April 2003.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-117 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1, 8-11, 44-45, 49, 82 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 17 August 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date <u>1/2003</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

CLAIMS PRESENTED

Claims 1-117 are presented.

CLAIM REJECTIONS

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1, 8-11, 44-45, 48, 82 are rejected under 35 U.S.C. 103(a) as being unpatentable over admitted prior art ("APA").

Regarding claim 1, APA teaches "A parallel encryption method for providing both data confidentiality and integrity for a message, comprising the steps of : receiving an input plaintext string comprising a message; generating a plurality of equal-sized blocks of t bits in length from the input plaintext string; creating an MDC block of t bits in length that includes the result of applying a non-cryptographic Manipulation Detection Code (MDC) function to the plurality of said equal-size blocks; presenting the equal-size blocks and the MDC block to a selected parallel encryption mode that makes one and only one processing pass with a single cryptographic primitive over each of the said equal-size blocks and said MDC block to create a plurality of hidden ciphertext blocks

Art Unit: 2134

each of t bits in length; and performing a hidden ciphertext randomization function over said plurality of hidden ciphertext blocks to create a plurality of output ciphertext blocks each of t bits in length (pages 1-13 of specification, especially the discussion on Jutla and previous works of Gligor which notes that such previous systems already had single pass situations, albeit not with both data confidentiality and integrity)."

These passages of APA do not teach the particular terminology and algorithm involving such "primitive" the sense of the claim.

Nevertheless, it was well known in the art to have a "primitive" for the motivation of cryptography.

Hence, it would have been obvious to those of ordinary skill in the art at the time of the claimed invention to modify APA for the motivation noted in the previous paragraphs so as to teach the claimed invention.

Regarding claims 8-11, 44-45, 48, 82 (and claim 1 as well), these claims merely state "both data confidentiality and integrity" in the preamble without specifically incorporate the features in the body of the claims. Thus, the claims must be read broadly. For the reasons noted in the APA at pages 1-13 of specification, especially the discussion on Jutla and previous works of Gligor which notes that such previous systems already had single pass situations, albeit not with both data confidentiality and integrity, these claims are not patentable. These passages of APA do not teach the particular terminology and algorithm involving such "primitive" the sense of the claim. Nevertheless, it was well known in the art to have a "primitive" for the motivation of cryptography. Hence, it would have been obvious to those of ordinary skill in the art at

Art Unit: 2134

the time of the claimed invention to modify APA for the motivation noted in the previous paragraphs so as to teach the claimed invention.

Allowable Subject Matter

All claims except claims 1, 8-11, 44-45, 48, 82 are allowed or allowable (upon being rewritten in proper form).

The following is a statement of reasons for the indication of allowable subject matter: the prior art did not teach or suggest such single pass and such use of primitive in the context of the other limitations of the claims so as to have both data confidentiality and integrity.

Conclusion

The art made of record and not relied upon is considered pertinent to applicant's disclosure. The art disclosed general background.

Points of Contact

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks

Washington, D.C. 20231

Art Unit: 2134

or faxed to:

(571) 273-8300, (for formal communications intended for entry)

Or:

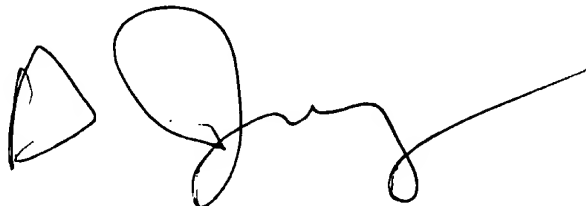
(571) 273-3836 (for informal or draft communications, please label "PROPOSED" or "DRAFT")

Any inquiry concerning this communication or earlier communications from the examiner should be directed to David Jung whose telephone number is (571) 272-3836 or Greg Morse whose telephone number is (571) 272-3838.

David Jung

Patent Examiner

10/3/05

A handwritten signature in black ink, consisting of a large, stylized 'D' followed by a series of loops and a long horizontal stroke extending to the right.